

Oracle® Healthcare Translational Research

Security Guide

Release 3.3

E93636-01

October 2018

Oracle Healthcare Translational Research (OHTR) allows you to pose meaningful questions, from a biological perspective, by combining clinical and cross-platform omics data. As a product, it also enables you to visualize clinical records and omics features using both in-house business intelligence tools, and omics viewers, developed by the research community.

Note: For the latest version of user documentation, head to Oracle Help Center.

This guide takes you through the guidelines of an OHTR installation. You can see the following topics below:

- [General Security Principles](#)
- [Security Guidelines for Database Objects and Database Options](#)
- [Disable unnecessary operating system level services](#)
- [Design Multiple Layers of Protection](#)
- [Security Guidelines for the Middle Tier](#)
- [Protect data](#)
- [Set up fine grain audit policy](#)
- [Documentation Accessibility](#)

1 General Security Principles

The following principles are fundamental to using any application securely.

1.1 Keep software up to date

One of the principles of good security practice is to keep all software versions and patches up to date. Ensure that you are current on CPUs.

1.2 Stay updated on the latest security information critical patch updates

Oracle continually improves its software and documentation. Critical Patch Updates are the primary means of releasing security fixes for Oracle products to customers with valid support contracts. They are released on the Tuesday closest to the 17th day of January, April, July and October. We highly recommend customers apply these patches as soon as they are released.

1.3 Configure strong passwords on the database

Although the importance of passwords is well known, the following basic rule of security management is worth repeating: **make sure your passwords are strong!**

You can strengthen passwords by creating and using password policies for your organization. For guidelines on securing passwords and for additional ways to protect passwords, see the specifics to the database release that you are using.

You should modify the following passwords to use your policy-compliant strings:

- Passwords for the database default accounts, such as SYS and SYSTEM.
- Passwords for the database application-specific schema accounts, such as HDM.
- Password for the database listener. You should not configure a password for the database listener as that will enable remote administration. For more information, see the *Removing the Listener Password* section of *Oracle® Database Net Services Reference 11g Release 2 (11.2)*

1.4 Follow the “principle of least privilege”

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Being overzealous with how you grant responsibilities and roles — especially early on in an organization's life cycle when people are few and work needs to be done quickly — often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine if they are still relevant for the current job responsibilities.

Create the database by following the steps listed in the *Oracle® Healthcare Translational Research Installation Guide*.

2 Security Guidelines for Database Objects and Database Options

This section describes security guidelines for OHTR's database objects and database options.

2.1 Oracle Healthcare Translational research objects

You can use DDL scripts and PL/SQL procedures and functions to create database objects and DML scripts to create seed data. These files are part of the media pack.

The guidelines for installing and configuring Oracle Database Server are available on Oracle Help Center, the Oracle Database 12c Release 2 page.

2.2 Oracle Database options

The Oracle Database has options that provide additional security features. OHTR may include data that falls under HIPAA guidelines in the United States and similar guidelines elsewhere. These features can help you comply with those guidelines.

Database Vault

Note: Database Vault requires a separate license.

With such sensitive data, only those with a valid need to know anything about it should have access to it. To prevent DBAs and others from seeing this data, it is recommended that Oracle Database Vault be used to limit users' access to the OHTR schema. This prevents prevent DBAs and other *superuser* accounts from accessing data.

Oracle Audit Vault

Note: Oracle Audit Vault requires a separate license.

Oracle Audit Vault automates the audit collection, monitoring, and reporting process, turning audit data into a key security resource for detecting unauthorized activity.

Consider using this feature to satisfy compliance regulations such as SOX, PCI, and HIPAA, and to mitigate security risks. OHTR sets the client identifier in the database session to allow identification of the end user.

Transparent Data Encryption

Transparent Data Encryption is one of the three components of the Oracle Advanced Security option for Oracle Database 12c Enterprise Edition. It provides transparent encryption of stored data to support your compliance efforts. If you employ Transparent Data Encryption, applications do not have to be modified and continue to work seamlessly as before. Data is automatically encrypted when it is written to disk and automatically decrypted when accessed by the application. Key management is built in, eliminating the complex task of creating, managing and securing encryption keys. Note that the Advanced Security Option is licensed separately from the database.

Tablespace Encryption

Tablespace Encryption is another component of the Oracle Advanced Security option for Oracle Database 12c Edition. Tablespace encryption facilitates encryption of the entire tablespace contents, rather than having to configure encryption on a column-by-column basis. It encrypts data at the data file level to keep users from viewing the Oracle data files directly. Oracle recommends that you perform tablespace encryption for maximum protection.

User Management

WebLogic Server supports several authentication security providers, for example, LDAP. For more information, see the *Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server* at

<http://docs.oracle.com/middleware/12212/wls/SECMG/conf-security-for-domain.htm#SECMG777>

OHTR supports any authentication security providers supported by WebLogic Server 12c (12.2.1.2).

Virtual Private Database

OHTR now uses Row Level Security (also referred to as Virtual Private Database or VPD) to store identifiable attributes. The policies created on the tables containing identifiable attributes are always controlled by policies to prevent any user from being able to query this information. The Row Level Security option used will return null values for any column value that a user does not have permission to view. OHTR now has views on all of these patient tables to use a NVL function on each identifiable

attribute to show an obfuscated value instead of the real value. If a user has permission to see the real value, then the real value will be returned in the view. Earlier versions of OHTR only showed obfuscated values and never stored real identifiable attributes.

There is an optional configuration to hide the rows of data that any user does not have permissions to view. By default this option is not enabled, meaning that users can query the data and see obfuscated values for all protected attributes. There is a default configuration that allows access to all identifiable data. Specific users that have proper credentials can be assigned access to this configuration. All control to the assignments of users is allowed to only users that have the VPD_ADMIN role assigned, and all calls use the CDM.VPD_UTIL package. For more information, see the *Oracle® Healthcare Translational Administrator's Guide*.

3 Disable unnecessary operating system level services

This section suggests various unused operating system level services that you can disable to improve security.

3.1 Disable the Telnet service

OHTR does not use the Telnet service.

Telnet listens on port 23 by default. If the Telnet service is available on any computer, Oracle recommends that you disable Telnet in favor of Transport Layer Security (TLS). Telnet, which sends clear-text passwords and user names through a log-in, is a security risk to your servers. Disabling Telnet tightens and protects your system security.

3.2 Disable other unused services

OHTR does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.
- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of OHTR. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

4 Design Multiple Layers of Protection

When designing a secure deployment, design multiple layers of protection. If a hacker should gain access to one layer, such as the application server, that should not automatically give them easy access to other layers, such as the database server.

Providing multiple layers of protection may include:

- Enabling only those ports required for communication between different tiers, for example, only allowing communication to the database tier on the port used for SQL*NET communications, (1521 by default).
- Placing firewalls between servers so that only expected traffic can move between servers.

5 Security Guidelines for the Middle Tier

This section describes the security guidelines for the OHTR middle tier.

5.1 Remove unused applications from WebLogic

Currently, the WebLogic Server installation includes the entire JDK and some additional WebLogic Server development utilities (for example, wlsvc). These development programs are not needed at runtime and can be safely removed. The following are recommendations for making a WebLogic Server installation more secure:

- Do not install the WebLogic Server sample applications.
- Delete development tools, such as the Configuration Wizard and the jCOM tools.
- Delete the Derby database, which is bundled with WebLogic Server for use by the sample applications and code examples as a demonstration database.

For more details, see the section on Determining Your Security Needs section in *Oracle® Fusion Middleware Securing a Production Environment for Oracle WebLogic Server 12c (12.2.1.2)* available at

<http://docs.oracle.com/middleware/12211/wls/LOCKD/practices.htm#LOCKD116>

5.2 Enable SSL/ TLS

To create a unique private identity key and trust certificate, TLS is not enabled by default during the installation. Enabling TLS is optional, but we recommend TLS for a production environment.

Note: Communication between the browser and the application servers should be restricted to TLS.

To enable Transport Layer Security:

1. Log into WebLogic Server Administration Console.
2. Click the **Environment** node in the Domain Structure pane and click **Servers** in the **Environment** table.
3. Click the server where you deployed the TrcApp.ear.
4. Click the **Configuration** tab.
5. Click the **General** tab.
6. If **Save** is disabled, click **Lock & Edit** in the **Change Center** pane.
7. Select the **SSL Listen Port Enabled** check box and enter a port number.
8. To disable non-SSL port, deselect the **Listen Port Enabled** check box.

9. Click **Save**.
10. Click **Activate Changes** in the **Change Center** pane, if it is enabled.
11. Click the **Control** tab.
12. Click the **Start/Stop** tab.
13. Click **Restart**
14. Click **Yes**.

The *TLS channels have been successfully restarted.* message appears.

You must also configure SSL, identity, and trust. For more information, see the *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c (12.2.1.2)*.

5.3 Configure SSL/ TLS

To set up TLS, perform the following steps:

1. Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for WebLogic Server.
Use the digital certificates, private keys, and trusted CA certificates provided by WebLogic Server, the CertGen utility, the keytool utility, or a reputable vendor such as Entrust or Verisign to perform this step.
2. Store the identity and trust. Private keys and trusted CA certificates which specify identity and trust are stored in keystores.
3. Configure the identity and trust keystores for WebLogic Server in the WebLogic Server Administration Console.
4. Set SSL configuration options for the private key alias and password in the WebLogic Server Administration Console. Optionally, set configuration options that require the presentation of client certificates (for two-way SSL).
5. Oracle Software Security standards recommend that you configure TLS 1.2. *weak SSL cyphers*, that is, TLS lower than v1.1 and SSL v3 and v2.

For further instructions on specifying the protocol and version, see the Specifying the SSL Protocol Version chapter in *Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server 12.2.1* available at

https://docs.oracle.com/middleware/1221/wls/SECMG/ssl_version.htm#SECMG636

For more details, see the section on Configuring SSL in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c (12.2.1.2)* available at

<https://docs.oracle.com/middleware/1221/core/ASADM/sslconfig.htm#ASADM1800>

5.4 Disable other unused services

OHTR does not use the following services or information for any functionality:

- Simple Mail Transfer Protocol (SMTP). This protocol is an Internet standard for E-mail transmission across Internet Protocol (IP) networks.
- Identification Protocol (identd). This protocol is generally used to identify the owner of a TCP connection on UNIX.
- Simple Network Management Protocol (SNMP). This protocol is a method for managing and reporting information about different systems.

- File transfer Protocol (FTP). This protocol is used for downloading or uploading files from the file server.

Therefore, restricting these services or information does not affect the use of OHTR. If you are not using these services for other applications, Oracle recommends that you disable these services to minimize your security exposure. If you need SMTP, identd, or SNMP for other applications, be sure to upgrade to the latest version of the protocol to provide the most up-to-date security for your system.

5.5 Protect user accounts

WebLogic Server defines a set of configuration options to protect user accounts from intruders. In the default security configuration, these options are set for maximum protection. You can use the Administration Console to modify these options on the **Configuration > User Lockout** page.

As a system administrator, you have the option of turning off all the configuration options, increasing the number of login attempts before a user account is locked, increasing the time period in which invalid login attempts are made before locking the user account, and changing the amount of time a user account is locked. Remember that changing the configuration options lessens security and leaves user accounts vulnerable to security attacks. For more details, see the section on Configuring Security for a WebLogic Domain section in *Oracle® Fusion Middleware Securing Oracle WebLogic Server 12c (12.2.1.2)* available at

<https://docs.oracle.com/middleware/1221/wls/SECMG/conf-security-for-domain.htm#SECMG777>

Monitor logs

If you suspect any unusual transactions in the Cohort UI, monitor the diagnostic logs for any real-time, abnormal business activity.

Application transactions should be monitored and real time corrective measures should be implemented to limit transaction rates outside application Service Level Agreements.

5.5.1 Password Validation Providers

WebLogic Server includes a Password Validation provider, which is configured by default in each security realm. The Password Validation provider manages and enforces a set of configurable password composition rules, and is automatically invoked by a supported authentication provider whenever a password is created or updated for a user in the realm. When invoked, the Password Validation provider performs a check to determine whether the password meets the criteria established by the composition rules. The password is then accepted or rejected as appropriate. For more information on the Password Validation provider, see the *Oracle® Fusion Middleware Administering Security for Oracle WebLogic Server 12c (12.2.1.2)* available at

https://docs.oracle.com/middleware/1221/wls/SECMG/password_atn.htm#SECMG206

6 Protect data

Data is vulnerable at many points in any computer system, and many security techniques and types of functionality can be employed to protect it.

7 Set up fine grain audit policy

The OHTR application has one schema:

- Application schema used by the OHTR application user interface

The following schemas from Oracle Healthcare Foundation (OHF) are used:

- Schema for Cohort Data Mart (CDM)
- Schema for Omics Data Bank (ODB)
- Application schema used by the Clinical Genomic APIs
- Enterprise Schema (ENT)

For details on setting up the audit policy for these schemas, see the *Oracle® Healthcare Foundation Security Guide*.

8 Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit

<http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Oracle Healthcare Translational Research Security Guide, Release 3.3
E93636-01

Copyright © 2013, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.